A1. Eve decides she wants to read Alice's mail, so she goes to the RSA public-key directory and finds Alice's keys, m_{ALICE} and e_{ALICE}. In order to find Alice's decryption key, Eve will have to factor m_{ALICE}, which is assumed to be the product of two primes.

Eve knows only one way to factor a number m: she tries dividing m by all the primes less than or equal to $\sqrt{m}$. Her computer can complete 100,000 of these trial divisions every second.

(a) Supppose that m_{ALICE} is approximately 3×10^{19} (that is, it's a twenty-digit number starting with 3). Approximately how long would it take Eve's computer to divide m_{ALICE} by all the primes up to $\sqrt{m_{\text{ALICE}}}$?

Solution: If $m_{\text{ALICE}} \approx 3 \times 10^{19}$, then $\sqrt{m_{\text{ALICE}}} \approx 5,500,000,000$.

By the Prime Number Theorem, there are approximately

$$\frac{5,500,000,000}{\ln 5,500,000,000} \approx 245,000,000$$

primes less than $\sqrt{m_{\text{ALICE}}}$. Trying these at the rate of $100,000$ primes per second, Eve's computer will have to work for about 2450 seconds, or about 41 minutes, to factor m_{ALICE}.

(b) Suppose Eve's computer program picks the trial divisors in a random order. Then she might get lucky and hit on one of the factors of m_{ALICE} right away. What is the probability that Eve's very first guess is one of the factors of m_{ALICE}?

Solution: Only one of the two factors of m_{ALICE} is less than $\sqrt{m_{\text{ALICE}}}$, so the probability of picking that number on the first try is about $1/245,000,000$. This is about the same as the probability of having a fair coin come up heads 28 times in a row.

(c) Now suppose $m_{\text{ALICE}} \approx 3 \times 10^{39}$ (that is, she uses a forty-digit number). How long will Eve's computer take to check all the possible prime divisors?

Solution: We have

$$\sqrt{m_{\text{ALICE}}} \approx 5.5 \times 10^{19},$$

which means Eve will have to check

$$\frac{5.5 \times 10^{19}}{\ln(5.5 \times 10^{19})} \approx 1.2 \times 10^{18}$$

primes. At 100,000 per second, it will take about 1.2×10^{13} seconds, or about $380,000$ years to try them all.

(d) How long will Eve's computer program take if $m_{\text{ALICE}} \approx 3 \times 10^{59}$?

Solution: We have

$$\sqrt{m_{\text{ALICE}}} \approx 5.5 \times 10^{59},$$

which means Eve will have to check

$$\frac{5.5 \times 10^{29}}{\ln(5.5 \times 10^{29})} \approx 8.0 \times 10^{27}$$

primes. At 100,000 per second, this will take about 8.0×10^{22} seconds, or about 2.5×10^{15} years.

A2. As we've seen in class, the number of digits in n_{ALICE} is usually the same as the number of digits in m_{ALICE}. When Alice uses a twenty-digit value for m_{ALICE}, it takes her computer about 1 second to run the extended Euclidean algorithm and find the value of d corresponding to any given e.

Alice is worried about security, and switches to a forty-digit value for m_{ALICE}. Based on your experience with the extended Euclidean algorithm, how long will it take Alice's computer to find the value of d corresponding to any given e?

How long will it take if m_{ALICE} has sixty digits?

Solution: The number of steps in the extended Euclidean algorithm seems to be roughly proportional to the number of digits in the larger of the two input numbers.

If the calculation takes one second on a twenty-digit number, it should take about two seconds on a forty-digit number, and about three seconds on a sixty-digit number.

Here's a page from the Factorville RSA Key Directory:

e_{ALICE}	=	34153	m_{ALICE}	=	243569
e_{BOB}	=	42713	m_{BOB}	=	339551
e_{CARL}	=	292811	m_{CARL}	=	321401

B1. (a) Alice receives four plaintext messages, each one with a digital signature attached. The plaintexts are 2003, 2004, 2005, and 2006. The complete, signed messages are

$$(2003, 116851), \quad (2004, 219536), \quad (2005, 288864), \quad (2006, 162131)$$

Each of the messages is either signed by Bob, signed by Carl, or is a forgery. Which is which?

Solution: We use the public keys for Bob and Carl to *encrypt* each of the signatures. We get

	$\sigma = 116851$	$\sigma = 219536$	$\sigma = 288864$	$\sigma = 162131$
$\sigma^{e_{\text{BOB}}}$ MOD m_{BOB}	1985	2004	196550	288702
$\sigma^{e_{\text{CARL}}}$ MOD m_{CARL}	254878	186609	2005	2006

The second message, 2004, is signed by Bob. The messages 2005 and 2006 are signed by Carl. The message 2003 does not have a valid signature on it.

(b) Suppose the forgery in B1a was actually a message from Bob that was intercepted and altered by Eve. What was Bob's intended message?

Solution: The signature on the message 2003 is what Bob would have signed for the message 1985.

B2. Eve, who spends all her time trying to defeat cryptographers, determines that m_{ALICE} is the product of the primes 373 and 653. She decides to impersonate Alice, by sending the message 1992 to Bob, with Alice's signature on it.

(a) What signature should Eve affix to the message 1992 in order to pretend to be Alice?

Solution: Eve must determine d_{ALICE}, for which she needs to know

$$\begin{aligned} n_{\text{ALICE}} &= 372 \times 652 \\ &= 242544. \end{aligned}$$

She then uses the extended Euclidean algorithm to find

$$\begin{aligned} d_{\text{ALICE}} &\equiv e_{\text{ALICE}}^{-1} \pmod{242544} \\ &\equiv 34153^{-1} \pmod{242544} \\ &\equiv 44137 \pmod{242544}. \end{aligned}$$

Now Eve knows how to sign Alice's name to anything. To the message 1992, she affixes the signature

$$\begin{aligned} \sigma &= 1992^{d_{\text{ALICE}}} \text{ MOD } m_{\text{ALICE}} \\ &= 1992^{44137} \text{ MOD } 243569 \\ &= 27932. \end{aligned}$$

(b) Eve encrypts her signed message using Bob's public key. What numbers does she send to Bob?

Solution: She uses e_{BOB} and m_{BOB} to encrypt both the plaintext and the signature. She gets

$$\begin{aligned} 1992^{e_{\text{BOB}}} \text{ MOD } m_{\text{BOB}} &= 1992^{42713} \text{ MOD } 339551 \\ &= 217865 \\ 27932^{e_{\text{BOB}}} \text{ MOD } m_{\text{BOB}} &= 27932^{42713} \text{ MOD } 339551 \\ &= 261002. \end{aligned}$$

Eve sends the encrypted pair $(217865, 261002)$.